



UNITED STATES PATENT AND TRADEMARK OFFICE

4/11

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/004,081	10/30/2001	David M. Blaker	9269-9	9375

20792 7590 01/11/2006

MYERS BIGEL SIBLEY & SAJOVEC'
PO BOX 37428
RALEIGH, NC 27627

EXAMINER

PICH, PONNOREAY

ART UNIT PAPER NUMBER

2135

DATE MAILED: 01/11/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/004,081	BLAKER, DAVID M.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 03 October 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-9 and 16-33 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-9 and 16-33 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>10/2005</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claims 1-9 and 16-33 are pending. Independent claims 1, 16, and 25 were amended. Any rejections or objections not repeated below for record are withdrawn due to applicant's amendments and/or arguments.

The examiner notes that the previous office action indicated that claims 4-5, 8-9, 19-20, 23-24, 28-29, and 32-33 recited subject matter allowable over the prior art. An updated search confirms this, however, the claims still contain 101 and 112 problems and are still rejected because applicant's amendments did not fix the 101 and there are new 112 problems, which were a result of applicant's amendments.

Information Disclosure Statement

Applicant's IDS submitted on 10/3/2005 has been considered.

Response to Arguments

The examiner notes that in response to the restriction requirements, applicant confirmed the election of claims 1-9 and 16-33 without prejudice or disclaimer.

In response to the 112 rejections in the previous office action, applicant stated that claims 3, 7, 18, 22, 27, and 31 were amended. The examiner notes that the claims are annotated as "currently amended", but no amendments were identified by applicant.

In response to the 101 rejections, applicant argues that claims 1 and 25 have been amended to indicate that the at least two sequential random values are determined for stream cipher, thus recites a useful, concrete, and tangible result. Applicant also states that claims 1 and 25 are not devoid of any limitation to a practical application in the technological arts as set forth in the MPEP. The examiner respectfully

Art Unit: 2135

disagrees with applicant. There are still 101 problems with the claims rejected under 35 USC 101 in the previous office action despite applicant's amendments. For claim 1, determining a random value is nothing more than a thought or computation in a computer. Contrary to applicant's arguments, the values are not applied/used in a stream cipher in the claimed method. Instead, they are merely determined with an intention of being used in a stream cipher as indicated by amended language "for the stream cipher". Claim 25 recites a computer program product comprising a computer readable media. In applicant's specification (see page 6, last paragraph), it appears that applicant intends for the media to cover signals. It is the Office's current view that signals do not constitute patent-eligible subject matter. Further, despite applicant's amendment, like claim 1, there lacks a useful, concrete, and tangible result recited in claim 25. Instead, "for the stream cipher" indicates intended use rather than actual use.

Applicant's art arguments were also considered, but are moot in view of new ground of rejections presented below. The examiner notes that applicant's amendments to the independent claims changed the scope of the claims.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 2-9 and 17-33 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Art Unit: 2135

1. Claim 2 recites “the step of determining at least two sequential random values in parallel utilizing a common S-box”, which lacks antecedent basis. Note applicant had amended this step in claim 1 so that it is now the step of “determining at least two sequential random values for the stream cipher in parallel utilizing a common S-box”.
2. Claim 17 recites “the means for determining at least two sequential random values in parallel utilizing the S-box”, which lacks antecedent basis. Note that applicant had amended this means in claim 16.
3. Claims 25 recites “computer readable program code configured to provide a memory”. It is unclear how code can provide memory.
4. Claim 26 recites “the computer readable program code configured to determine at least two sequential random values in parallel utilizing the S-box”, which lacks antecedent basis. Note that applicant had amended this computer readable program code in claim 25.
5. Any claims not specifically addressed are rejected by virtue of dependencies.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-9 and 25-33 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 1:

As per claim 1, determining a random value is nothing more than a thought or computation in a computer. Claim 1 reads on a method implemented with software alone and does not require any physical structure for the implementation of the method. Further, the method does not recite any tangible result. Note “for the stream cipher” indicates intention of use rather than actual use of the random values. Intended use does not yield tangible results. This 101 rejection can be overcome if applicant recites a limitation indicating the determined values actually being used in a stream cipher or otherwise recites a practical application of at least one of the values.

Claims 2-9:

Claims 2-9 are dependent on claim 1 and merely further defines the software determining step of claim 1. As such, claims 2-9 are also directed towards non-statutory subject matters since they too do not recite any useful, concrete, and tangible result.

Claim 25:

Claim 25 refers to a computer program product comprising a computer readable media. The examiner notes that on page 6, lines 31-33, applicant defines a computer-readable medium as including “an electronic, magnetic, optical, electromagnetic, infrared, or semiconductor system, apparatus, device, or propagation medium.” As such, the computer-readable media recited in claim 25 reads on a signal. It is the Office’s current view that signals do not constitute patent-eligible subject matter. Claim 25 also does not recite any tangible result. The examiner notes that if applicant did not define a computer readable storage media as a signal in the specification, the computer

Art Unit: 2135

program product of claim 25 comprising a computer readable storage media and the code being configured to provide a useful, concrete, and tangible result would be statutory.

Claims 26 and 27:

Claims 26 and 27 merely further define the computer readable program code recited in claim 25 and still do not recite any statutory subject matter.

Claim 28:

Claim 28 further defines the computer readable program code recited in claim 25. In addition, claim 28 also recites at least two software states and a software counter. Nothing statutory was recited.

Claims 29-31:

Claims 29-31 merely further define the computer readable program code recited in claim 25 and still do not recite any statutory subject matter.

Claim 32:

Claim 32 further defines the computer readable program code recited in claim 25. In addition, claim 32 also recites at least two software states and a software counter. Nothing statutory was recited.

Claims 33:

Claim 33 merely further defines the computer readable program code recited in claim 25 and still does not recite any statutory subject matter.

Claim Rejections - 35 USC § 103

Art Unit: 2135

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 16, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Venkatesan et al (US 6,490,354) in view of Yoshida (US 5,434,807).

Claim 1:

Venkatesan discloses the limitation of determining at least two sequential random values for the stream cipher utilizing a common S-box (Fig 6; col 9, lines 31-57; and col 11, lines 22-25).

Venkatesan does not explicitly disclose the determining is done in parallel. However, the examiner asserts that determining (random) values in parallel was well known in the art at the time applicant's invention was made. Yoshida discloses determining of random numbers is done in parallel (col 2, lines 65-68).

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify Venkatesan's invention such that the determining was done in parallel. One of ordinary skill would have been motivated to do so because parallel processing allows more results to be obtained faster than if it was done sequentially.

Claims 16 and 25:

Claims 16 and 25 recite limitations substantially similar to claim 1. The difference is that claim 16 refers to a system and claim 25 refers to a computer program product

Art Unit: 2135

with means and computer readable media having computer readable program code therein, the computer readable program code comprising computer readable program code configured to implement the method of claim 1.

Another difference is that claims 16 and 25 explicitly recite a memory containing an S-box, which is also implicitly disclosed by Venkatesan (col 10, line 8-col 11, line 5).

Claims 2-3, 6-7, 17-18, 21-22, 26-27, and 30-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Venkatesan et al (US 6,490,354) in view of Yoshida (US 5,434,807) and further in view of Klug et al (US 5,528,526).

Claims 2, 17, and 26:

Claims 17 and 26 are substantially similar to claim 2. Claim 17 differs from claim 2 in that claim 17 recites a system with means for implementing the method of claim 2. Claim 26 differ in that it recites a computer program product with computer readable program code for implementing the method of claim 2.

As per claims 2, 17, and 26, Venkatesan further discloses accesses of the common S-box utilized to determine a first of the two sequential random values and access of the common S-box utilized to determine a second of the two sequential random values (Fig 6; col 9, lines 31-57; and col 11, lines 22-25). Venkatesan's invention is used with a stream cipher, so the numbers in the stream of numbers generated by Venkatesan's random number generator are all random numbers.

Venkatesan does not disclose:

1. Determining if a collision exists between accesses.
2. Modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the common S-box.

However, Klug discloses determining if a collision/cycle exists between in the generation of random numbers (col 3, lines 21-35). Note that each symbol disclosed by Klug in the pattern supplied on bus 18 reads on a random number. In light of this, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to have modified Venkatesan's invention to determine if a collision exists between accesses of the common S-box utilized to determine a first of the two sequential random values and access of the common S-box utilized to determine a second of the two sequential random values. One of ordinary skill would have been motivated to do so as Klug discloses that by detecting short cycle patterns (collisions), many diverse failure modes associated with random number generators may be identified.

Klug also does not explicitly disclose modifying the determination of the at least two sequential random values based on whether a collision exists between accesses of the common S-box. However, this limitation is obvious to the combination of Venkatesan and Klug as the reason Klug wanted to detect collision or repeating patterns in random number generation was to determine if an error is present in the generation process. If an error is present, it is obvious to one of ordinary skill to modify

Art Unit: 2135

the determination of the random values as recited in claims 2, 17, and 26. One of ordinary skill would have been motivated to modify the determination, as it would correct the errors disclosed by Klug.

Claims 6, 21, and 30:

Claims 21 and 30 are substantially similar to claim 6. Claim 21 differs from claim 6 in that claim 21 recites a system with means for implementing the method of claim 6. Claim 30 differ in that it recites a computer program product with computer readable program code for implementing the method of claim 6.

As per claims 6, 21, and 30, Venkatesan does not disclose:

1. Determining if a collision exists between accesses of the common S-box utilized to determine a first portion of the first of the two sequential random values and accesses of the common S-box utilized to determine a second portion of the first of the two sequential random values.
2. Determining if a collision exists between accesses of the common S-box utilized to determine a first portion of the second of the two sequential random values and accesses of the common S-box utilized to determine a second portion of the two sequential random values.

However, the above limitations are obvious to the combination of Venkatesan, Yoshida, and Klug. Venkatesan's invention deals with generating a stream of random numbers (in byte format) for encryption purposes (col 1, lines 9-12). Klug deals with detecting collisions or pattern repeats within a sequence of numbers/symbols (col 1,

Art Unit: 2135

lines 8-12). It is obvious that the combination invention of Venkatesan, Yoshida, and Klug would be able to detect collisions within any random value comprising a first and second portion as the combination invention looks for collisions within the streams itself rather than just one number with another number. The examiner also notes that within the stream generated, it is arbitrary where one "number" begins and ends as it depends on the system the random number generator is used how many bits or bytes comprise a number.

Claims 3, 7, 18, 22, 27, and 31:

Venkatesan does not explicitly disclose:

1. Determining a state associated with the determination of the at least two sequential random values.
2. Comparing values of counters utilized in determining the at least two sequential random values.
3. Detecting a collision based on the determined state and the compared values.

However, the above limitations are obvious to the combination invention of Venkatesan, Yoshida, and Klug. Klug discloses that once a collision is first detected, more tests are needed to determine if the collision is a false repeat or not (Fig 2; Fig 5; and col 6, line 45-col 7, line 40). Each level of testing for a match reads on a separate state as disclosed by Klug. To determine absolutely that the pattern detected is not a false collision, the state must be determined to be the final level of verification (Fig 5, items 82 and 84).

Allowable Subject Matter

Claims 4-5, 8-9, 19-20, 23-24, 28-29, and 32-33 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 101 and 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

Claims 4, 19, and 28:

The examiner did not find teachings in the prior art *wherein the step of detecting a collision comprises the steps of:*

1. *Detecting a first collision if the determined state is the first state and the second i counter values equals the first j counter value.*
2. *Detecting a collision if the determined state is the first state and the second j counter value equals the first i counter value.*
3. *Detecting a third collision if the determined state is the first state and the second j counter values equals the first j counter value.*
4. *Detecting a fourth collision if the determined stat is the second state, the second j counter values equals the first t counter value.*

Art Unit: 2135

5. *Detecting a fifth collision if the determined state is the second state and the second t counter values equals the first i counter value and the second j counter value is not equal to the first i counter value.*

Claims 8, 23, and 32:

The examiner did not find teachings in the prior art wherein *determining if a collision exists...comprises the steps of:*

1. *Detecting a first collision if the determined state is the second state and the first i counter value equals the first t counter value.*
2. *Detecting a second collision if the determined state is the second state and the second t counter value equals the second i counter value.*

Claims 5, 9, 20, 24, 29, and 33:

Claims 5, 9, 20, 24, 29, and 33 depends on claims that were indicated as allowable above.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the

Art Unit: 2135

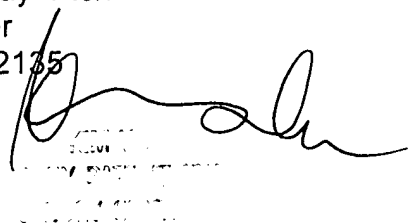
shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ponnoreay Pich
Examiner
Art Unit 2135

A handwritten signature in black ink, appearing to read 'P. Pich', is written over a faint, rectangular official stamp. The signature is fluid and cursive.

PP